UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,329	11/23/2001	Stefano Faccin	017.39681X00	3557

20457	7590	03/11/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER
SONG, HOSUK

ART UNIT	PAPER NUMBER
2135	8

DATE MAILED: 03/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No. 09/990,329	Applicant(s) FACCIN ET AL.
Office Action Summary	Examiner Hosuk Song	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _23 November 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-44_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-17,27-42,44_ is/are rejected.

7)☒ Claim(s) _18-26 and 43_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _23 November 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _5,7_.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public
use or on sale in this country, more than one year prior to the date of application for patent in the United
States.

1.   Claims 1-3,5-8,10-11,27-29,32,35-38,40-41,44 are rejected under 35 U.S.C. 102(b) as

being anticipated by Ohashi(EP 0673178 A2).

Claim 1: Ohashi discloses generating a first key for a mobile node in (col.3,lines 13-20).

Ohashi discloses storing the first key at the mobile node and at a home domain of the mobile

node in (fig.5A,S501 and S502). Ohashi disclose moving the mobile node to the second domain

in (fig.5A,roamed network). Ohashi discloses sending a request from the second domain to the

home domain to authenticate the mobile node in (fig.2b). Ohashi discloses generating a second

key at the home domain using the first key and a random number and sending the random

number and the second key to the second domain in (fig.2b,S214,S215,S216). Ohashi

discloses sending the random number to the mobile node by the second domain in (fig.6,#64).

Ohashi discloses generating the second key by the mobile node using the random number and

the first key in (fig.6,#602). Ohashi discloses using the second key for at least one

authentication procedure between the mobile node and the second domain in (fig.6,S603).

Claim 2: Ohashi discloses second domain is a visited domain (fig.2a).

Claim 3: Ohashi discloses authentication procedure is a key derivation procedure in

(fig.2b,S214,S215).

Claim 5: Ohashi discloses authentication procedure comprise authentication of the

mobile node by the second domain in (fig.6,S603).

Claim 6: Ohashi discloses authentication procedures comprises authentication of the

second domain by the mobile node in (fig.5a). Note that mutual authentication is achieved

between mobile and seond domain in fig.5a.

Claim 7: Ohashi discloses second domain controls key distribution between the mobil

node and entities in the second domain in (fig.6).

Claim 8: Ohashi discloses ciphering and integrity protection of messages between node

and an entity in the second domain in (fig.5a).

Claim 10: Ohashi discloses generating the second key at the home domain using the

first key and the random numbers as inputs to an algorithm in (fig.5a). note that home network

generates second key and the random number using a function.

Claim 11: Ohashi discloses sending the random number and the second key to the

second domain across a secure channel in (fig.5a) note secure communication line between

mobile and roamed network.

Claim 27: Ohashi discloses sharing a first key with a mobile node and at least one server

in the home domain of the mobile node and moving the mobile node into the second domain in

(fig.2b). Ohashi discloses requesting authentication of the mobile node by the home domain in

(fig.2a). Ohashi discloses generating a second key using the first key in the home domain in

(fig.2b,S215). Ohashi discloses sending the second key to the second domain (fig.2b). Ohashi

discloses using the second key for at least one authentication procedure between the mobile

node and the second domain in (fig.2b,S216) a security association existing between the one at

least one server in the home domain and one at least one second server in the second domain

in (col.2,lines 50-58 and col.3,lines 1-12) wherein when the mobile device roams into the

second domain, the second domain requests authentication of the mobile device by the home

domain in (fig.2b and col.3,lines 13-35). One at least one server generating a second key using

the first key and sending the second key to the second domain, the second key being used for

at least one authentication procedure between the mobile device and the second domain in

(fig.2b and col.3,lines 13-35).

Claim 28: Ohashi discloses second domain is a visited domain (fig.2a).

Claim 29: Ohashi discloses a home domain containing at least one server in (fig.2b).

Ohashi discloses a mobile device (fig.12A), the mobile device sharing a first key with one at

least one server in the home domain in (fig.12A,S1202). Ohashi discloses a second domain the

second domain containing at least one second server (fig.12A).

Claim 32: Ohashi discloses mobile device comprises a mobile phone in (col.1,lines 1-

25).

Claim 35: Ohashi discloses authentication procedure comprise authentication of the

mobile node by the second domain in (fig.6,S603).

Claim 36: Ohashi discloses authentication procedures comprises authentication of the

second domain by the mobile node in (fig.5a). Note that mutual authentication is achieved

between mobile and seond domain in fig.5a.

Claim 37: Ohashi discloses second domain controls key distribution between the mobil

node and entities in the second domain in (fig.6).

Claim 38: Ohashi discloses ciphering and integrity protection of messages between

node and an entity in the second domain in (fig.5a).

Claim 40: Ohashi disclose moving the mobile node to the second domain in

(fig.5A,roamed network). Ohashi discloses sending a request from the second domain to the

home domain to authenticate the mobile node in (fig.2b). Ohashi discloses generating a second

key at the home domain using the first key and a random number and sending the random

number and the second key to the second domain in (fig.2b,S214,S215,S216). Ohashi

discloses sending the random number to the mobile node by the second domain in (fig.6,#64).

Ohashi discloses generating the second key by the mobile node using the random number and

the first key in (fig.6,#602). Ohashi discloses using the second key for at least one

authentication procedure between the mobile node and the second domain in (fig.6,S603).

Claim 41: Ohashi discloses moving a mobile node comprising a mobile phone to the

second domain in (fig.2a and col.1 lines 1-25).

Claim 44: Ohashi discloses second domain is a visited domain (fig.2a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 4,34,42 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ohashi(EP 0673178 A2) in view of Schneier(Applied Cryptography).

Claims 4,34,42: Ohashi does not specifically discloses generating at least one session

key using the second key. Schneier discloses key exchange protocol using a session key in

(page 33, section on session key generation). It would have been obvious to person of ordinary

skill in the art at the time invention was made to employ a session key as taught in Schneier

with key derivation method disclosed in Ohashi so that one key is used for one communication

and then discarded and if some key exchange protocol to transfer the key from one conversant

to the other, the key does not have to be stored before it is used. This makes it far less likely

that the key might be compromised.

3.   Claims 12-16,30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ohashi(EP0673178 A2) in view of Verma et al(US 6,522,880).

Claims 12-16,30-31: Ohashi does not specifically discloses home domain comprises an

Authentication Authorization and Accounting (AAA) server. Verma's patent teaches AAA server

in (col.2,lines 55-67;col.3,lines 1-16). It would have been obvious to person of ordinary skill in

the art at the time invention was made to employ AAA server as taught in Verma with system

disclosed in Ohashi in order to load off some of the processing and memory requirements from

the second domain and further facilitates management, accounting and authentication issues for

the provider of the network.

4.   Claims 17,33 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ohashi(EP 0673178 A2) in view of Brown et al.(US 5,668,875).

Claims 17,33: Ohashi does not specifically discloses temporary shared key(TSK).

Brown's patent discloses generating TSK in mobile communication network in (col.4,lines 17-

23). It would have been obvious to person of ordinary skill in the art at the time invention was

made to generate a TSK as taught in Brown with key generator disclosed in Ohashi in order to

minimize the need for inter network traffic and since the key is temporary, key does not have to

be stored for long duration where it is vulnerable for key attacks thus minimizing key

compromise.

5.   Claims 9,39 rejected under 35 U.S.C. 103(a) as being unpatentable over Ohashi(EP

0673178 A2) in view of Dent(5,091,942).

Claims 9,39: Ohashi does not specifically disclose distribution of dynamic keys between

the mobile device and entities in the second domain based on a local security association.

Dent's patent discloses this features in (col.20,lines 54-63). It would have been obvious to

person of ordinary skill in the art at the time invention was made to employ a dynamic keys as

taught in Dent with key derivation method disclosed in Ohashi so that session cipher key does not need to be programmed into device or the network infrastructure before device goes into service. If or when security has or have been compromised the cipher key can be dynamically changed when requested wither by the user or the network operator thus enhancing security of its keys against hackers.

Allowable Subject Matter

6.   Claims 18-26,43 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim 18: prior art of record does not teach generating a third key at the home domain using the first key and the second random number and sending random number and the third key to the second domain.

Claims 19-25 are allowed because of dependency.

Claim 26: prior art of record does not teach generating second authentication data using the host challenge and the first key at the home domain and sending the second authentication data from the home domain to the second domain,the second domain forwarding the second authentication data to the mobile node and using the second authentication data to verify the home domain by the mobile node.

Claim 43: prior art of record does not teach sending a third key from the home domain to the second domain, the third key being based on the first key; authenticating the second domain by the mobile device using the third key and updating the second key with the third key at the mobile device,third key is used for the authentication procedures.
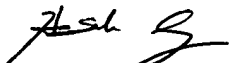
Conclusion

7.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner

can normally be reached on Tue-Fri from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS